TheHive Nedir?

TheHive, güvenlik olaylarının yönetimine ve analizine yardımcı olmak için tasarlanmış açık kaynaklı ve ücretsiz bir Güvenlik Olayı Müdahale Platformudur (SIRP). SOC'ler, CSIRT'ler, CERT'ler, hızla araştırılması ve harekete geçilmesi gereken güvenlik olaylarıyla ilgilenen tüm bilgi güvenliği uygulayıcılarının hayatını kolaylaştırmak için tasarlanmıştır. Güvenlik analistleri, Bilgisayar Güvenliği Olay Müdahale Ekipleri (CSIRT'ler) ve Güvenlik Operasyon Merkezleri (SOC'ler) için geliştirilen TheHive, tehdit avcıları ve olaylara müdahale edenlerin güvenlik olaylarını verimli ve etkili bir şekilde araştırmaları ve çözmeleri için kapsamlı bir çözüm sunar.

Özelleştirilebilir gösterge tabloları, yerleşik gözlemlenebilir veriler, MISP ve Cortex gibi popüler tehdit istihbaratı araçlarıyla entegrasyon dahil olmak üzere zengin özellikleriyle TheHive, güvenlik uzmanlarının, güvenlik olaylarını etkili ve verimli bir şekilde önceliklendirmesine, analiz etmesine ve bunlara yanıt vermesine olanak tanır. TheHive, Cortex, güvenlik analistleri ve araştırmacılar gözlemlenebilir ögeyi kolaylıkla analiz edebilir.

Revision #10
Created 7 April 2024 11:30:32 by Güldeniz Akca
Updated 13 April 2024 13:20:43 by Güldeniz Akca